

PR-9



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,351	06/29/2001	Joubert Berger	10013502-1	2270

7590 05/07/2004

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P. O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER
----------

KENDALL, CHUCK O

ART UNIT	PAPER NUMBER
----------	--------------

2122

DATE MAILED: 05/07/2004

9

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/896,351

Applicant(s)

BERGER ET AL.

Examiner

Chuck O Kendall

Art Unit

2122

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 0.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-39 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-39 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.  
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4,5. 6) ☐ Other: \_\_\_\_\_

Art Unit: 2122

### DETAILED ACTION

1. This action is in response to the application filed 02/18/04.
2. Claims 1 – 39 have been examined.

### Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,10,11,13 –18 & 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Drake et al. USPN 6,347,374 B1.

Regarding claim 1, a system comprising:

operating system providing at least one routine capable of being invoked, and said operating system operable to collect audit data for invoked operating system routines (FIG.1, 26);

data storage having collected audit data stored thereto in a first format and software code executable by at least one processor to receive said collected audit data and generate output comprising at least a portion of said collected audit data in a desired for-mat defined by a template, wherein said desired format is different than said first format (FIG.1, 38, see destination dir and parameter, for format also see 2: 45 – 55, also see storage mechanism).

Regarding claim 10, the system of claim 1 wherein said template comprises at least one conditional element (2: 45 – 55, see compare, misuse engine and output mechanism).

Art Unit: 2122

Regarding claim 11, the system of claim 10 wherein said at least one conditional element dictates that said output is to have a particular format if a condition is satisfied otherwise said output is to have a different format (7: 25 - 31).

Regarding claim 13, the system of claim 1 wherein said operating system comprises a kernel-level audit device driver for collecting said audit data (9:55 – 60, see collector for different operating system for kernel level device driver).

Regarding claim 14, the product version of the system in claim 1, see rationale as previously discussed above.

Regarding claim 15, the computer program product of claim 14 wherein said audit data is collected by an operating system (9:55 – 60).

Regarding claim 16, the computer program product of claim 14 wherein said at least one routine includes at least one invoked operating system routine (9:55 – 60, see collector).

Regarding claim 17, the computer program product of claim 16 wherein said at least one invoked operating system routine is invoked by an application via system call (10:51 – 57).

Regarding claim 18, the computer program product of claim 16 wherein said at least one invoked operating system routine is invoked via user command (8:25 – 35).

Regarding claim 37, the software version of the system in claim 1, see rationale as previously discussed above.

### **Claim Rejections - 35 USC § 103**

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the

Art Unit: 2122

invention was made.

6. Claims 2 – 9, 19 – 36, 38 & 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over in view of Drake et al. USPN 6,347,374 as applied in claim 1, in view of Sutton et al. USPN 5,920,719.

Regarding claim 2, Drake discloses all the claimed limitations as applied in claim 1. Drake doesn't explicitly disclose wherein said template comprises at least one constant element. Sutton discloses abstract as well as variable primitives allowing the user to extend data types used for information collection (9: 30 – 35). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Drake and Sutton because, using constant elements ensures more reusability of templates.

Regarding claim 3, the system of claim 2 wherein said at least one constant is included in verbatim in said output (Drake, 4: 5 – 10).

Regarding claim 4, Drake discloses all the claimed limitations as applied in claim 1. Drake doesn't explicitly disclose wherein said template comprises at least one variable element. Sutton discloses abstract as well as variable primitives allowing the user to extend data types used for information collection (9: 30 – 35). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Drake and Sutton because, using variable elements would make the templates more customizable.

Regarding claim 5, the system of claim 4 wherein said at least one variable element identifies a particular portion of the collected audit data to be included in said output (Drake, 4:3 – 25).

Regarding claim 6, wherein said at least one variable element identifies a particular portion of the collected audit data to be included in said output (Drake, 4:3 – 25).

Regarding claim 7, the system of claim 1 wherein said collected audit data comprises a record for each invocation of an operating system routine that is included within said collected audit data, and wherein each record includes at least one type of audit information relating to execution of an invoked operating system routine (Drake, Col.9: 20 – 35).

Art Unit: 2122

Regarding claim 8, the system of claim 7 wherein said at least one type of audit information includes at least one type selected from the group consisting of:

user identification, group identification, supplementary group identification, process identification, event identification, event count, event type, date, time, thread identification, system call, capabilities used, object, and result (Drake 5, 40 – 55).

Regarding claim 19, the product version of the system in claim 3, see rationale as previously discussed above.

Regarding claim 20, the product version of the system in claim 4, see rationale as previously discussed above.

Regarding claim 21, the product version of the system in claim 7, see rationale as previously discussed above.

Regarding claim 22, the product version of the system in claim 8, see rationale as previously discussed above.

Regarding claim 23, the computer program product of claim 22 wherein said audit data comprises multiple ones of said record, further comprising code executable to sort at least a portion of the multiple records based on at least one of said types of audit information (Drake, 4: 20 – 24, see filter for sort).

Regarding claim 24, the product version of the system in claim 9, see rationale as previously discussed above.

Regarding claim 25, the product version of the system in claim 10, see rationale as previously discussed above.

Regarding claim 26, the method version of the system in claim 4, see rationale as previously discussed above.

Regarding claim 27, the method version of the product in claim 4, see rationale as previously discussed above.

Regarding claim 28, the method of claim 26 further comprising the step of creating, by a user, said audit transformation template (Drake, 16: 1 – 7).

Art Unit: 2122

Regarding claim 29, the method version of the system in claim 3, see rationale as previously discussed above.

Regarding claim 30, the method version of the system in claim 4, see rationale as previously discussed above.

Regarding claim 31, the method version of the system in claim 5, see rationale as previously discussed above.

Regarding claim 32, the method version of the system in claim 8, see rationale as previously discussed above.

Regarding claim 33, the method of claim 26 further comprising the step of: presenting said output to a user (Drake, 4:3 – 25).

Regarding claim 34, the method version of the system in claim 5, see rationale as previously discussed above.

Regarding claim 35, the method of claim 26 further comprising the step of inputting said output to an application for processing by said application (Drake, 4:3 – 25).

Regarding claim 36, the method of claim 26 further comprising the step of: sorting said collected audit data based at least in part on at least one type of audit information included therein (Drake, 17: 30 – 32, see filter and sort templates]).

Regarding claim 38, the software version of the system in claim 5, see rationale as previously discussed above.

Regarding claim 39, the library of claim 37 wherein said function executable to access collected audit data, said function executable to access a template, and said function executable to generate output are included within a common function (Drake, 21: 7 – 11).

Regarding claim 9, see reasoning in claim 4.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Drake et al. USPN 6,347,374 as applied in claim 1, in view Maloney et al. USPN 6,253,337 B1.

Art Unit: 2122

Regarding claim 12, Drake discloses all the claimed limitations as applied in claim 1. Drake doesn't expressly disclose wherein said template defines a format of a markup language. However, Maloney does disclose this feature in a similar configuration. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Drake with Maloney to implement the instant claimed invention because, use of the HTML format would made the system more distributed and internet compatible.

### Correspondence Information

7. Any inquires concerning this communication or earlier communications from the examiner should be directed to Chuck O. Kendall who may be reached via telephone at (703) 308-6608. The examiner can normally be reached Monday through Friday between 8:00 A.M. and 5:00 P.M. est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Dam *can be* reached at (703) 305-4552.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

*For facsimile (fax) send to 703-7467239 official and 703-7467240 draft*

*Chuck O. Kendall*

Software Engineer Patent Examiner  
United States Department of



**TUAN DAM**  
**SUPERVISORY PATENT EXAMINER**